PAT-NO: JP02002086970A

DOCUMENT-IDENTIFIER: JP 2002086970 A

TITLE: CAT TERMINATORY MACHINE

PUBN-DATE: March 26, 2002

INVENTOR-INFORMATION:

NAME	COUNTRY
ARAI, CHIHARU	N/A
OMORI, HIROYOSHI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NEC INFRONTIA CORP	N/A

APPL-NO: JP2000276707

APPL-DATE: September 12, 2000

INT-CL (IPC): B42D015/10, G06K017/00

ABSTRACT:

PROBLEM TO BE SOLVED: To prevent the illicit acquisition of **card** data and the use of unlawful **cards** from developing.

SOLUTION: In the case 35c of a magnetic head 35, a demodulation circuit 37 for demodulating **card** data on the receipt of the output signal of a magnetic head main body and an encipherment circuit 38 for enciphering the demodulated **card** data are provided. At the same time, the image data of a character line train displayed by embossing on the surface of the magnetic **card** 1 are **detected with an embossed** character sensor 40. Then, the enciphered data is decoded by a decoding means 47. The character data string corresponding to the character string displayed by embossing on the basis of the image data is obtained by a character recognizing means 48 so as to judge whether the data string in the predetermined bit range of the decoded **card** data coincides with the character data string or not by a judging means 49. Only when the data trains are judged to be coincided with each other, a communication for authentication is performed to the predetermined center.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－86970
（P2002－86970A）
(43)公開日　平成14年３月26日(2002.3.26)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｂ４２Ｄ　15/10	５０１	Ｂ４２Ｄ　15/10	５０１Ｌ	２Ｃ００５
			５０１Ｐ	５Ｂ０５８
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ａ	
			Ｓ	

審査請求　未請求　請求項の数２　ＯＬ　（全８頁）

(21)出願番号　特願2000－276707(P2000－276707)

(22)出願日　平成12年９月12日(2000.9.12)

(71)出願人　000227205
エヌイーシーインフロンティア株式会社
神奈川県川崎市高津区北見方２丁目６番１号

(72)発明者　荒井　千春
東京都港区南麻布五丁目10番27号　アンリツ株式会社内

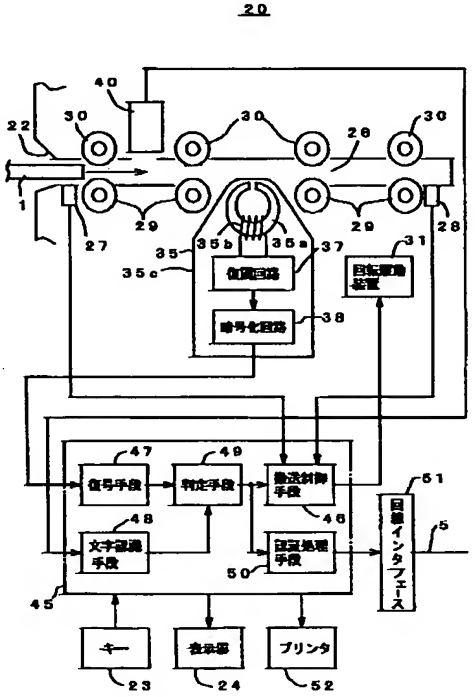
(72)発明者　大森　宏祥
東京都港区南麻布五丁目10番27号　アンリツ株式会社内

(74)代理人　100079337
弁理士　早川　誠志

最終頁に続く

(54)【発明の名称】　ＣＡＴ端末機

(57)【要約】
【課題】　カードデータの不正取得と、不正なカードの利用を防止する。
【解決手段】　磁気ヘッド３５のケース３５ｃ内に、磁気ヘッド本体の出力信号を受けてカードデータを復調する復調回路３７と、復調されたカードデータを暗号化する暗号化回路３８とを設けるとともに、磁気カード１の表面にエンボス加工によって表示されている文字列のイメージデータをエンボス加工文字センサ４０によって検出する。そして、暗号化されたデータを復号手段４７によって復号し、イメージデータに基づいてエンボス加工によって表示されている文字列に対応するキャラクタデータ列を文字認識手段４８によって求め、復号されたカードデータの所定ビット範囲のデータ列とキャラクタデータ列とが一致するか否かを判定手段４９によって判定し、データ列が一致すると判定されたときのみ、所定のセンタに対して認証のための通信を行う。



1

【特許請求の範囲】
【請求項1】磁気カードをカード挿入口から筐体内に受け入れ、前記磁気カードに磁気記録されているカードデータを磁気ヘッドを用いて再生し、該カードデータを含む情報を通信回線を介して所定のセンタに送信して認証を受けるCAT端末機において、
前記磁気ヘッドのケース内に設けられ、磁気ヘッド本体の出力信号を受けて前記カードデータを復調する復調手段と、
前記磁気ヘッドのケース内に設けられ、前記復調手段によって復調されたカードデータを暗号化して前記ケースの外部へ出力する暗号化手段と、
前記磁気ヘッドのケースの外部に出力されたデータを復号する復号手段と、
前記筐体内に受け入れた磁気カードの表面にエンボス加工によって凹凸で表示されている文字列のイメージデータを検出するエンボス加工文字センサと、
前記エンボス加工文字センサによって検出されたイメージデータに基づいて、前記エンボス加工によって凹凸で表示されている文字列に対応するキャラクタデータ列を求める文字認識手段と、
前記復号手段によって復号されたカードデータの所定ビット範囲のデータ列と、前記文字認識手段によって求められたキャラクタデータ列とが一致するか否かを判定する判定手段と有し、
前記判定手段によって前記カードデータの所定ビット範囲のデータ列と前記キャラクタデータ列とが一致すると判定されたときのみ、前記所定のセンタに対して認証のための通信を行うように構成されていることを特徴とするCAT端末機。
【請求項2】少なくとも前記復号手段と判定手段とが1チップ化された単一のプロセッサによって構成されていることを特徴とする請求項1記載のCAT端末機。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、クレジットカード等の磁気カードに対する認証処理を行うためのCAT端末機において、磁気カードのデータが不正に取得されたり、不正なカードの利用を防止するための技術に関する。
【0002】
【従来の技術】店舗等でクレジットカードによる支払いを行う場合に、その店舗に設けられたCAT端末機を用いている。
【0003】CAT端末機は、挿入されたクレジットカードに磁気記録されているカードデータを読み取り、所定のセンタへ送信してそのカードの利用が可能か否かの認証を受けている。
【0004】図6は、このような目的で使用される従来のCAT端末機10の概略構成を示している。

2

【0005】このCAT端末機10は、図示しない筐体の表面に設けられたカード挿入口11から挿入された磁気カード1を内部に引き込んで所定の搬送路12に沿って搬送し、この搬送路12に設けられた磁気ヘッド13によって磁気カード1の磁気記録面の磁気変化を検出し、この検出信号を復調回路14に入力して磁気カード1に磁気記録されているカードデータを復調する。
【0006】復調されたカードデータを受けた処理部15は、このカードデータを含む情報を回線インタフェース16および通信回線5を介して所定のセンタ（図示せず）へ送信して認証を受ける。
【0007】
【発明が解決しようとする課題】しかしながら、上記のように構成された従来のCAT端末機10では、磁気ヘッド13の出力ラインや復調回路14の出力ラインに対する不正なアクセスによって磁気カード1のカードデータを不正に取得される恐れがある。
【0008】また、このように不正に取得されたカードデータを別の磁気カードに書き込んで作成された不正カードが利用される恐れがある。
【0009】本発明は、この問題を解決して、カードデータが不正に取得されたり、不正なカードの利用を防止できるCAT端末機を提供することを目的としている。
【0010】
【課題を解決するための手段】前記目的を達成するために、本発明の請求項1のCAT端末機は、磁気カードをカード挿入口から筐体内に受け入れ、前記磁気カードに磁気記録されているカードデータを磁気ヘッドを用いて再生し、該カードデータを含む情報を通信回線を介して所定のセンタに送信して認証を受けるCAT端末機において、前記磁気ヘッドのケース内に設けられ、磁気ヘッド本体の出力信号を受けて前記カードデータを復調する復調手段と、前記磁気ヘッドのケース内に設けられ、前記復調手段によって復調されたカードデータを暗号化して前記ケースの外部へ出力する暗号化手段と、前記磁気ヘッドのケースの外部に出力されたデータを復号する復号手段と、前記筐体内に受け入れた磁気カードの表面にエンボス加工によって凹凸で表示されている文字列のイメージデータを検出するエンボス加工文字センサと、前記エンボス加工文字センサによって検出されたイメージデータに基づいて、前記エンボス加工によって凹凸で表示されている文字列に対応するキャラクタデータ列を求める文字認識手段と、前記復号手段によって復号されたカードデータの所定ビット範囲のデータ列と、前記文字認識手段によって求められたキャラクタデータ列とが一致するか否かを判定する判定手段と有し、前記判定手段によって前記カードデータの所定ビット範囲のデータ列と前記キャラクタデータ列とが一致すると判定されたときのみ、前記所定のセンタに対して認証のための通信を行うように構成されている。

【００１１】また、本発明の請求項２のＣＡＴ端末機は、請求項１のＣＡＴ端末機において、少なくとも前記復号手段と判定手段とが１チップ化された単一のプロセッサによって構成されている。

【００１２】

【発明の実施の形態】以下、図面に基づいて本発明の実施の形態を説明する。図１は本発明を実施したＣＡＴ端末機２０の外観を示し、図２はその内部構成を示している。

【００１３】図１に示しているように、このＣＡＴ端末機２０の筐体２１の前面側には、クレジットカードなどの磁気カード１を挿入するためのカード挿入口２２が設けられ、筐体２１の上面側には、テンキー等を含む複数のキー２３、表示器２４および後述するプリンタ５２の排紙口２５が設けられている。

【００１４】また、筐体２１の内部には、図２に示しているように、カード挿入口２２と連続し、カード挿入口２２から挿入された磁気カード１を筐体２１内で略水平に搬送させるための搬送路２６が形成されている。

【００１５】この搬送路２６の前端および後端には、磁気カードのエッジを検出するためのセンサ２７、２８が設けられている。

【００１６】また、搬送路２６には、磁気カードを両面から挟んだ状態で搬送路２６に沿って搬送させるためのローラ２９、３０が複数組設けられ、例えばその下方側のローラ２９（上方側のローラ３０でもよい）が図示しないベルト等によって同方向に回転するように連結され、そのうちの少なくとも一つのローラ２９がモータを含む回転駆動装置３１に連結されている。

【００１７】搬送路２６の中間部で磁気カードの磁気記録帯が通過する位置には、磁気ヘッド３５が配置されている。この磁気ヘッド３５は、ギャップを有するコア３５ａにコイル３５ｂが巻かれた本体部を、磁気シールド用の金属製のケース３５ｃ内に収容しており、このケース３５ｃの表面に露呈するコア３５ａのギャップ部分で磁気カード１の磁気記録帯の磁気変化を検出し、その磁気変化に対応する信号をコイル３５ｂから出力する。

【００１８】磁気ヘッド３５のコイル３５ｂから出力される信号は復調回路３７に入力される。復調回路３７は、磁気ヘッド３５のコイル３５ｂから出力される信号から磁気カード１に磁気記録されているカードデータを復調する。

【００１９】なお、このカードデータの復調は、磁気カード１に対するデータの記録方式に対応しており、例えばその記録方式が一般的なＭＦＭ方式（Ｆ２Ｆ方式ともいう）の場合には、磁気ヘッド３５の本体部（コア３５ａ、コイル３５ｂ）からの出力信号を増幅し、その信号の半サイクル周期が基準周期に近いか基準周期の２倍に近いかを判定することによってカードデータを復調する。

【００２０】復調回路３７によって復調されたデータは暗号化回路３８に入力される。暗号化回路３８は、復調回路３７によって復調されたデータを所定の暗号化関数と鍵データとによって暗号化する。この暗号化は、例えば、暗号化対象データに対する鍵データとの排他的論理和演算処理、暗号化対象データに対する鍵データによって指定されたビット位置の置換処理、暗号化対象データに対する鍵データによって指定されたビット数のシフト処理の組み合わせによって行う。

【００２１】上記復調回路３７および暗号化回路３８は、磁気ヘッド３５の本体部分とともに磁気ヘッド３５のケース３５ｃ内に収容され、ケース３５ｃの内部の隙間には合成樹脂が充填されており、暗号化回路３８によって暗号化されたデータがケース３５ｃの外部へ出力される。

【００２２】なお、図示していないが、復調回路３７および暗号化回路３８には、ケース３５ｃの外部から電源が供給できるようになっている。

【００２３】したがって、このケース３５ｃから外部に出力されるデータを不正に取得しても、内部の暗号化回路３８の暗号化関数や鍵データがわからないので、磁気カード１に記録されているカードーデータを容易に知ることはできない。

【００２４】また、搬送路２６には、磁気カード１の表面にエンボス加工によって凹凸で表示された文字（数字や記号も含む）のイメージデータを取得するためのエンボス加工文字センサ４０が設けられている。

【００２５】このエンボス加工文字センサ４０は、非接触型、接触型のいずれでもよい。ただし、非接触型のうち、ＣＣＤ素子等でエンボス加工部分を正面から撮像してそのイメージデータを検出しようとすると、エンボス加工部分の汚れやインクのかすれ等によって正しいカードと判定されない恐れがあるので、エンボス加工による凹凸を光学的に検出する必要がある。

【００２６】例えば図３のエンボス加工文字センサ４０のように、磁気カード１の表面に光を照射する投光器４１と、投光器４１から磁気カード１の平坦部分に照射されて反射する光を集光するレンズ４２と、集光レンズ４２で集光された光を受光する受光器４３とを一組のセンサ素子とし、このセンサ素子を磁気カード１の搬送方向に直交する方向に複数並べて構成し、投光器４１からの光が磁気カード１の平坦部に照射している場合にはレンズ４２が集光した光が受光器４３で受光され、投光器４１からの光が磁気カード１のエンボス加工による突起部分２に照射している場合にはレンズ４２が集光した光が受光器４３の受光面から外れるようにし、各受光器４３の受光信号を２値化してイメージデータとして出力する。

【００２７】また、接触型のものとしては、例えば図４に示すエンボス加工文字センサ４０のように、自重ある

いはバネによって下方へ付勢された状態で上下動（または回動）できるように支持したピン状の接触子４４をその磁気カード１の搬送方向と直交する方向に複数配置して構成し、各接触子４４毎に、その接触子４４が磁気カード１の平坦面に下端を当接している状態か、磁気カード１のエンボス加工による突起部分２に下端が乗り上げている状態かを判定するための判定器（図示せず）を設け、これらの判定器の出力をイメージデータとして出力する。

【００２８】なお、この判定器としては、接触子４４に連結されその上下動（または回動）によって開閉するスイッチや、接触子４４の上端に押されその押圧力に対応した信号を出力する圧力センサや、接触子４４の高さや傾きによって遮光状態から受光状態に切り換わる投受光素子等を用いることができる。

【００２９】センサ２７、２８、暗号化回路３８およびエンボス加工文字センサ４０の出力は、処理部４５に入力される。

【００３０】処理部４５は、１チップ化されたマイクロプロセッサによって構成されており、その機能をブロック化すると、図２に示しているように、搬送制御手段４６、復号手段４７、文字認識手段４８、判定手段４９および認証処理手段５０を備えている。

【００３１】この処理部４５には、複数のキー２３、表示器２４、回線インタフェース５１、プリンタ５２が接続されており、回線インタフェース５１および通信回線５を介して所定のセンタとの間でキー２３からの入力情報やカードデータ等を含む情報の授受を行い、表示器２４にキー２３の入力情報やセンタとの通信に関わる情報等を表示し、プリンタ５２から決済結果等が印字された紙を出力させる。

【００３２】図５は、処理部４５の処理手順を示すフローチャートである。以下、このフローチャートに基づいてこのＣＡＴ端末機２０の動作を説明する。

【００３３】磁気カード１がカード挿入口２２に挿入されて、その先端がセンサ２７で検知されると、搬送制御手段４６は、各ローラ２９が引込方向に回転するように回転駆動装置３１を駆動し、磁気カード１を搬送路２６に沿って奥側に搬送させる（Ｓ１、Ｓ２）。

【００３４】そして、この磁気カード１の引込搬送が開始されると、文字認識手段４８はエンボス加工文字センサ４０からのイメージデータの取得を開始し、復号手段４７は、暗号化回路３８からのデータの取得を開始する（Ｓ３）。

【００３５】そして、磁気カード１の先端がセンサ２８で検出されると、搬送制御手段４６は、回転駆動装置３１を停止させ、磁気カード１の搬送を一時停止する（Ｓ４、Ｓ５）。

【００３６】ここで、文字認識手段４８は、取得したイメージデータに基づいて、磁気カード１の表面にエンボス加工によって凹凸で表示された文字のキャラクタデータを求める（Ｓ６）。なお、この文字認識処理は磁気カード１の引込搬送中に行ってもよい。

【００３７】また、復号手段４７は取得した暗号化データを復号して磁気カード１に記録されていたカードデータを求める（Ｓ７）。なお、この復号処理は磁気カード１の引込搬送中に行ってもよい。

【００３８】そして、判定手段４９は、文字認識手段４８によって求められたキャラクタデータ列と復号手段４７によって求められたカードデータとを照合し、カードデータの所定ビット範囲のデータ列がキャラクタデータ列に一致するか否かを判定する（Ｓ８）。

【００３９】一般にエンボス加工によって文字列が表示されている磁気カードでは、その文字列に対応するキャラクタデータ列が磁気記録データに含まれているので、上記の判定を行うことで、その磁気カードが使用可能なカードか否かを判定することができる。

【００４０】ここで、カードデータの所定ビット範囲のデータ列がキャラクタデータ列に一致する場合には、この磁気カード１は正しいカードであるとし、認証処理手段５０によるカードデータの認証や決済等の処理（前記センタとの通信を含む）がなされた後、搬送制御手段４６によって磁気カード１が返却される（Ｓ９、Ｓ１０）。

【００４１】また、カードデータの所定範囲のデータ列がキャラクタデータ列に一致しない場合には、この磁気カード１が不正に作成されたものとし、前記認証処理を行わずにその磁気カードを返却する。

【００４２】なお、カードデータの所定範囲のデータ列がキャラクタデータ列に一致しない場合に、カードデータの読み取りとエンボス加工文字のイメージデータの取得とを所定回数まで繰り返してデータ判定を行い（前記Ｓ２～Ｓ８の処理を繰り返す）、データが一致した時点で、その磁気カード１を正しいカードとして処理し、所定回数連続して一致しない場合にその磁気カード１を不正に作成されたカードとして返却するようにしてもよい。

【００４３】このように、実施の形態のＣＡＴ端末機２０では、磁気ヘッド３５のケース３５ｃ内に復調回路３７および暗号化回路３８が収容されているので、磁気カード１のカードデータが磁気ヘッド３５の出力ラインから不正に取得される恐れがなく、しかも、磁気カード１エンボス加工によって凹凸で表示された文字列のキャラクタデータ列とカードデータの所定ビット位置のデータ列との一致を判定し、一致したときのみセンタとの間の認証処理を行うようにしているので、不正に取得されたカードデータを書き込んだ不正なカードの利用を確実に防ぐことができる。

【００４４】また、前記したように、カードデータを入出力する復号手段４７と判定手段４９とを含む処理部４

5が1チップ化された単一のプロセッサによって構成されているので、磁気カード1のカードデータをこの処理部45から不正に取得される恐れがなく、カードデータの不正取得に対する安全性がさらに高くなる。

【0045】

【発明の効果】以上説明したように、本発明の請求項1のCAT端末機は、磁気カードをカード挿入口から筐体内に受け入れ、前記磁気カードに磁気記録されているカードデータを磁気ヘッドを用いて再生し、該カードデータを含む情報を通信回線を介して所定のセンタに送信して認証を受けるCAT端末機において、前記磁気ヘッドのケース内に設けられ、磁気ヘッド本体の出力信号を受けて前記カードデータを復調する復調手段と、前記磁気ヘッドのケース内に設けられ、前記復調手段によって復調されたカードデータを暗号化して前記ケースの外部へ出力する暗号化手段と、前記磁気ヘッドのケースの外部に出力されたデータを復号する復号手段と、前記筐体内に受け入れた磁気カードの表面にエンボス加工によって凹凸で表示されている文字列のイメージデータを検出するエンボス加工文字センサと、前記エンボス加工文字センサによって検出されたイメージデータに基づいて、前記エンボス加工によって凹凸で表示されている文字列に対応するキャラクタデータ列を求める文字認識手段と、前記復号手段によって復号されたカードデータの所定ビット範囲のデータ列と、前記文字認識手段によって求められたキャラクタデータ列とが一致するか否かを判定する判定手段と有し、前記判定手段によって前記カードデータの所定ビット範囲のデータ列と前記キャラクタデータ列とが一致すると判定されたときのみ、前記所定のセンタに対して認証のための通信を行うように構成されている。

【0046】このように、磁気ヘッドのケース内に復調手段および暗号化手段が収容されているので、磁気カードのカードデータが磁気ヘッドの出力ラインから不正に取得される恐れがなく、しかも、磁気カードのエンボス加工によって凹凸で表示された文字列のキャラクタデータ列とカードデータの所定ビット位置のデータ列との一致を判定し、一致したときのみセンタとの間で認証処理を行うようにしているので、不正に取得されたカードデータを書き込んだ不正なカードの利用を確実に防ぐことができる。

【0047】また、本発明の請求項2のCAT端末機は、請求項1のCAT端末機において、少なくとも前記復号手段と判定手段とが1チップ化された単一のプロセッサによって構成されている。

【0048】このため、復号されたカードデータを不正に取得することができず、カードデータの不正取得に対する安全性がさらに高くなる。

【図面の簡単な説明】

【図1】本発明の実施の形態の外観を示す斜視図

【図2】本発明の実施の形態の内部構成を示す図

【図3】本発明の実施の形態の要部の構成例の概略図

【図4】本発明の実施の形態の要部の別の構成例の概略図

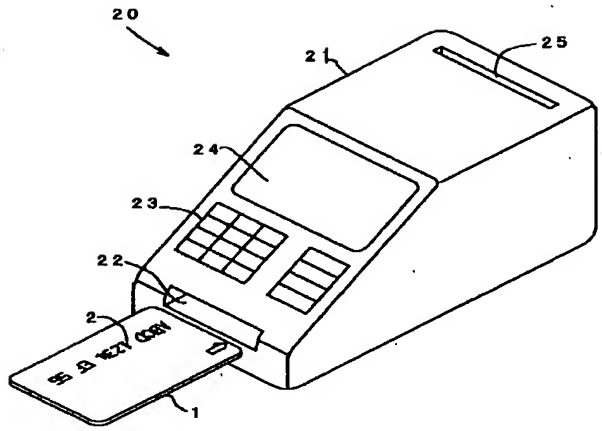
【図5】本発明の実施の形態の要部の処理手順を示すフローチャート

【図6】従来装置の構成を示す図

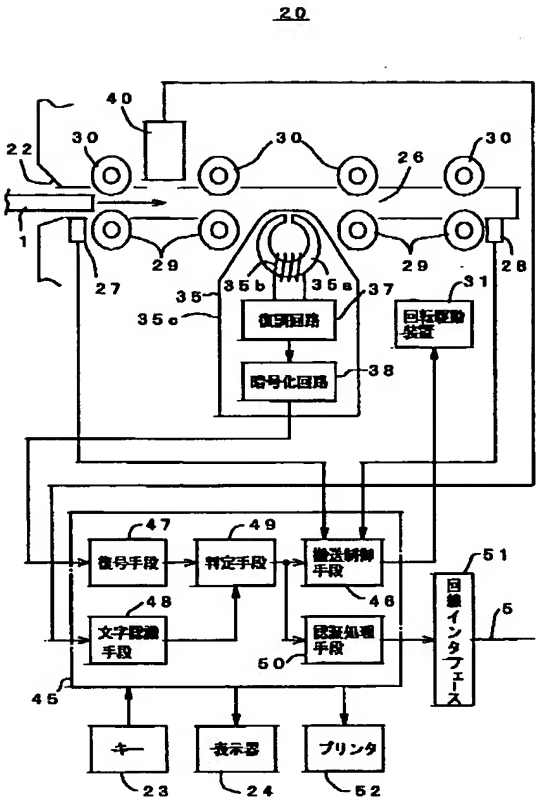
【符号の説明】

1　磁気カード
2　エンボス加工による突起部分
5　通信回線
20　CAT端末機
21　筐体
22　カード挿入口
23　キー
24　表示器
25　排紙口
26　搬送路
27、28　センサ
29、30　ローラ
31　回転駆動装置
35　磁気ヘッド
35a　コア
35b　コイル
35c　ケース
37　復調回路
38　暗号化回路
40　エンボス加工文字センサ
41　投光器
42　レンズ
43　受光器
44　接触子
45　処理部
46　搬送制御手段
47　復号手段
48　文字認識手段
49　判定手段
50　認証処理手段
51　回線インタフェース
52　プリンタ

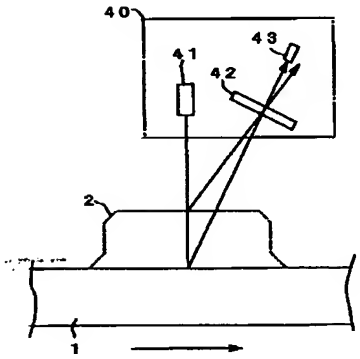
【図1】


20
21
25
24
23
22
2
1

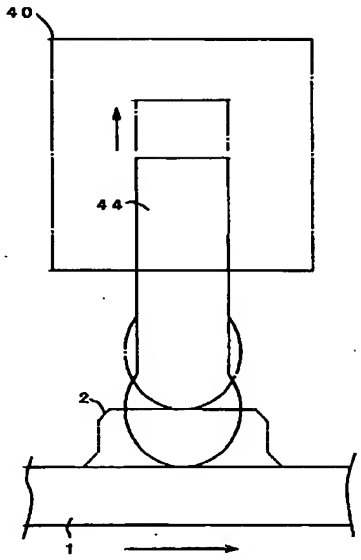
【図2】


20
40
30
30
26
30
22
1
29
29
28
27
35
35b
35a
37
31
35c
復調回路
回転駆動装置
暗号化回路
38
47
49
51
復号手段
判定手段
搬送制御手段
48
46
文字認識手段
回転処理手段
50
5
回線インタフェース
45
キー
表示器
プリンタ
23
24
52

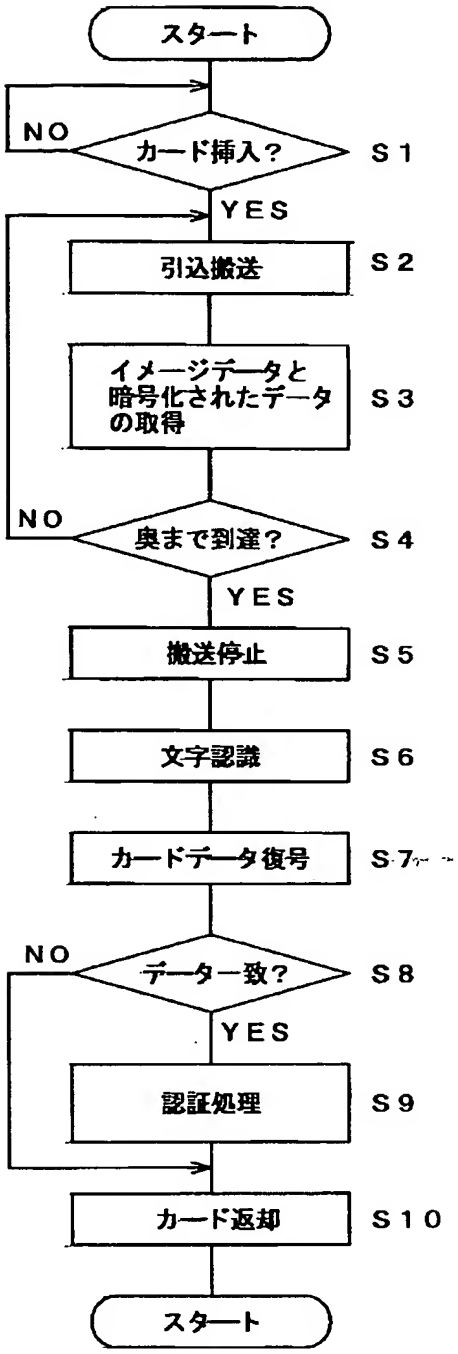
【図3】


40
41
43
42
2
1

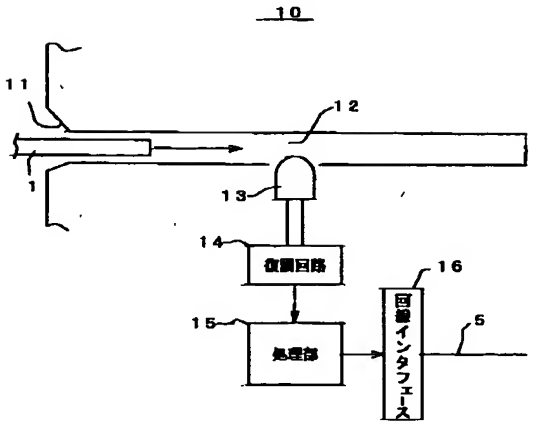
【図4】


40
44
2
1

【図5】


スタート
NO
カード挿入？
S１
YES
引込搬送
S２
イメージデータと
暗号化されたデータ
の取得
S３
NO
奥まで到達？
S４
YES
搬送停止
S５
文字認識
S６
カードデータ復号
S７
NO
データー致？
S８
YES
認証処理
S９
カード返却
S１０
スタート

【図6】


10
11
12
1
13
14
復調回路
16
15
処理部
回線インタフェース
5

フロントページの続き

Fターム(参考)　2C005 HA01 JA01 JA08 JB31 LB02
LB04 LB15 LB18 LB34
5B058 CA31 CA35 KA02 KA04 KA08
KA35 YA20